(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 061 514 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
20.12.2000 Bulletin 2000/51

(51) Int. Cl.[7]: **G11B 20/00**, G06F 1/00

(21) Application number: **00112708.3**

(22) Date of filing: **15.06.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **16.06.1999 JP 17018799**

(71) Applicants:
- **KABUSHIKI KAISHA TOSHIBA**
  Kawasaki-shi (JP)
- **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.**
  Kadoma-shi, Osaka (JP)

(72) Inventors:
- **Kamibayashi, Tooru,**
  K.K.Toshiba,
  Intell Prop. Div.
  Tokyo 105-8001 (JP)
- **Yamada, Hisashi,**
  K.K.Toshiba,
  Intell Prop. Div.
  Tokyo 105-8001 (JP)
- **Iwasaki, Hiroshi,**
  K.K.Toshiba,
  Intell Prop. Div.
  Tokyo 105-8001 (JP)
- **Tamura, Masafumi,**
  K.K.Toshiba,
  Intell Prop. Div.
  Tokyo 105-8001 (JP)
- **Ishibashi, Yasuhiro,**
  K.K.Toshiba,
  Intell Prop. Div
  Tokyo 105-8001 (JP)
- **Kato, Taku,**
  K.K.Toshiba,
  Intellectual Prop. Div.
  Tokyo 105-8001 (JP)
- **Tatebayashi, Makoto**
  Takarazuka-shi, Hyogo-ken (JP)
- **Harada, Shunji**
  Nishinari-ku, Osaka-shi, Osaka-fu (JP)

(74) Representative:
Henkel, Feiler, Hänzel
Möhlstrasse 37
81675 München (DE)

(54) Mutual authentication method, recording apparatus, reproducing apparatus, and recording medium

(57) In a mutual authentication method for use between a recording apparatus which records copied contents on a recording medium having an arithmetic processing function, and the recording medium, the method includes a step of storing in the recording medium at least first information (MID) which depends on the recording medium, and second information (SMID) which is to be shared by the recording apparatus in executing mutual authentication with the recording apparatus and depends on the recording medium, and a step of generating by the recording apparatus authentication information (K_M[MID]) used in mutual authentication with the recording medium on the basis of the first information (MID) obtained from the recording medium, and executing mutual authentication between the recording apparatus and the recording medium using the generated authentication information (K_M[MID]) and the second information (SMID).

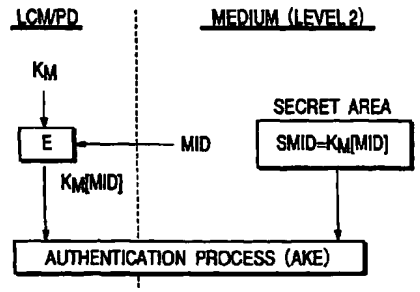

FIG. 8B

EP 1 061 514 A2

Description

[0001] The present invention relates to a mutual authentication method for use among a recording apparatus, reproducing apparatus, and recording medium, using a contents management technique that protects copyrights by limiting the number of copied contents, and a recording apparatus, reproducing apparatus, and recording medium using the method.

[0002] Conventionally, contents (literary works and the like) have undergone copy management. More specifically, by managing copy generations or the number of copies, copyright protection and use are balanced.

[0003] On the other hand, the concept "move" has appeared as an alternative to copy management. "Copy" does not erase original data, but "move" transfers data to another location (recording medium) and erases original data. As a result, a protection technique against "move" has appeared. Such technique has emerged due to digitalization of contents and prevalence of networks and the like.

[0004] However, in recent years, since copies faithful to an original can be formed via the network or the like, it becomes difficult for the conventional technique to reliably protect copyrights. Particularly, it is hard to reliably protect copyrights against unlimited moves from medium to medium, e.g., profit-making distribution (by means of move) of data.

[0005] It is an object of the present invention to provide a mutual authentication method which can assure high information security between a recording medium and a recording apparatus that records copied contents on the recording medium, and between a recording medium and a reproducing apparatus which reproduces copied contents recorded on the recording medium, and a contents recording apparatus, reproducing apparatus, and recording medium using the method.

[0006] According to one aspect of the present invention, there is provided a mutual authentication method for use between a recording apparatus which records copied contents on a recording medium having an arithmetic processing function, and the recording medium, the method comprising the steps of: storing in the recording medium at least first information which depends on the recording medium, and second information which is to be shared by the recording apparatus in executing mutual authentication with the recording apparatus and depends on the recording medium; and generating by the recording apparatus authentication information used in mutual authentication with the recording medium on the basis of the first information obtained from the recording medium, and executing mutual authentication between the recording apparatus and the recording medium using the generated authentication information and the second information.

[0007] According to another aspect of the present invention, there is provided a mutual authentication method for use between a reproducing apparatus which reproduces copied contents recorded on a recording medium having an arithmetic processing function, and the recording medium, the method comprising the steps of: storing in the recording medium at least first information which depends on the recording medium, and second information which is to be shared by the reproducing apparatus in executing mutual authentication with the reproducing apparatus and depends on the recording medium; and generating by the reproducing apparatus authentication information used in mutual authentication with the recording medium on the basis of the first information obtained from the recording medium, and executing mutual authentication between the reproducing apparatus and the recording medium using the generated authentication information and the second information.

[0008] According to still another aspect of the present invention, there is provided a recording apparatus for recording copied contents on a recording medium while limiting the number of copied contents to be recorded on the recording medium; the apparatus comprising: generation means for generating authentication information, which is used in mutual authentication with the recording medium and is to be shared by the recording medium, on the basis of first information which is obtained from the recording medium and depends on the recording medium; and mutual authentication means for executing mutual authentication with the recording medium using the authentication information generated by the generation means.

[0009] According to still another aspect of the present invention, there is provided a reproducing apparatus for reproducing copied contents recorded on a recording medium while limiting the number of copied contents to be recorded on the recording medium, the apparatus comprising: generation means for generating authentication information, which is used in mutual authentication with the recording medium and is to be shared by the recording medium, on the basis of first information which is obtained from the recording medium and depends on the recording medium; and mutual authentication means for executing mutual authentication with the recording medium using the authentication information generated by the generation means.

[0010] According to still another aspect of the present invention, there is provided a recording medium having an arithmetic processing function, comprising: storage means for pre-storing first information which is unique to the recording medium, and second information which is to be shared by a recording apparatus for recording copied contents on the recording medium and a reproducing apparatus for reproducing the copied contents in executing mutual authentication among the recording medium, the recording apparatus, and the reproducing apparatus, and depends on the recording medium; and mutual authentication means for executing mutual authentication between the recording

medium and the recording apparatus, and between the recording medium and the reproducing apparatus using authentication information generated based on the first information by the recording apparatus and the reproducing apparatus, and the second information.

[0011] This summary of the invention does not necessarily describe all necessary features so that the invention may also be a sub-combination of these described features.

[0012] The invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a block diagram showing an example of the arrangement of a music contents use management system (LCM) using a contents management technique for limiting the number of copied contents that can be recorded on a recording medium according to an embodiment of the present invention;

FIG. 2 shows an example of the map of a memory area;

FIG. 3 is a block diagram showing an example of the internal arrangement of a recording/reproducing device (PD);

FIGS. 4A to 4C are views for explaining the features of three different recording media;

FIG. 5 is a block diagram showing an example of the internal arrangement of a medium interface (I/F);

FIG. 6 is a view for explaining the recorded contents of a recording medium after check-in;

FIGS. 7A to 7C show storage examples of guest books stored in a secret area of an LCM;

FIGS. 8A and 8B are views for explaining an outline of a mutual authentication method;

FIG. 9 is a flow chart for explaining a check-in/check-out process sequence;

FIG. 10 is a chart for explaining a sequence of check-out when the type of recording medium is level 2;

FIG. 11 is a chart for explaining a sequence of reproduction when the type of recording medium is level 2;

FIG. 12 is a chart for explaining a sequence of check-in when the type of recording medium is level 2;

FIG. 13 is a chart for explaining another sequence of check-out when the type of recording medium is level 2;

FIG. 14 is a chart for explaining another sequence of reproduction when the type of recording medium is level 2;

FIG. 15 is a chart for explaining a sequence of check-out when the type of recording medium is level 0;

FIG. 16 is a chart for explaining a sequence of reproduction when the type of recording medium is level 0;

FIG. 17 is a chart for explaining a sequence of check-in when the type of recording medium is level 0;

FIG. 18 is a chart for explaining another sequence of check-out when the type of recording medium is level 0;

FIG. 19 is a chart for explaining another sequence of reproduction when the type of recording medium is level 0;

FIG. 20 is a chart for explaining another sequence of check-in when the type of recording medium is level 0;

FIG. 21 is a chart for explaining processing operation of a mutual authentication process (AKE); and

FIG. 22 is a chart for explaining another processing operation of a mutual authentication process (AKE).

[0013] An embodiment of the present invention will be explained hereinafter with reference to the accompanying drawings.

[0014] FIG. 1 shows an example of the arrangement of a music contents use management system (to be also simply referred to as an LCM hereinafter) which limits the number of copied contents that can be recorded on a recording medium according to this embodiment, and records copied contents on a medium, reproduces copied contents recorded on a medium, and so forth. Note that music is used as an example of contents. However, the present invention is not limited to such specific contents, and movies, game software programs, and the like may be used. A memory card (MC) is used as a medium. However, the present invention is not limited to such medium, and various other recording media such as a floppy disk, DVD, and the like may be used.

[0015] An EMD (Electronic Music Distributor) is a music distribution server or music distribution broadcast station.

[0016] A contents use management system 1 is, for example, a personal computer (PC), which includes receivers #1 to #3 corresponding to a plurality of EMDs (EMD#1 to EMD#3 in this case), and receives encrypted contents, their licenses (the use condition and decryption key Kc for the encrypted contents), and the like distributed by the EMDs. Receivers #1 to #3 may have a reproducing function or a charging function. The user uses the reproducing function to listen to samples of the distributed music contents. Also, the user can purchase the contents he or she likes using the charging function.

[0017] The LCM 1 includes a secure contents server (Secure Music Server: SMS in this case; to be also simply referred to as an SMS hereinafter) 2, and the contents the user has purchased are stored in the SMS 2 via an EMD interface (I/F) 3. The music contents are decrypted by the EMD I/F 3 as needed, and

undergo format conversion and re-encryption. Upon receiving the encrypted contents, the SMS 2 stores the received contents in a music data memory 10, and a music data decryption key in a license memory 9. The SMS 2 may have a reproducing function. With this reproducing function, the music contents managed by the SMS 2 can be reproduced on the PC.

[0018] The SMS 2 has a function of outputting contents data to a medium (to be also simply referred to as an MC (memory card) hereinafter) 13. The user can reproduce the contents recorded on the MC 13 by setting it in a recording/reproducing device (to be also simply referred to as a PD (Portable Device) hereinafter.

[0019] The SMS 2 records contents on the MC 13 directly via a medium (MC) interface 6 or with the intervention of the PD 12.

[0020] A device ID memory 4 includes, e.g., a ROM which stores identification information (device ID) of the LCM.

[0021] The MC 13 has identification information (MID) which is unique to that medium and cannot be rewritten, and the contents stored in the MC 13 may be encrypted by an encryption key which depends on the MC 13.

[0022] A check-in/check-out process will be explained first using the LCM 1 shown in FIG. 1.

[0023] The check-out process means making a copy of "parent" contents stored in the LCM 1 on the MC 13 as "child" contents. The "child" contents can be freely reproduced by the PD 12, but it is not allowed to form "grandchild" contents from the "child". The number of "children" "parent" can have is defined as an attribute of "parent". On the other hand, the check-in process means erasing (or disabling to use) "child" contents by the LCM 1 when the MC 13 is connected to the LCM 1, thereby recovering the right of "parent" contents in the LCM 1 to form one "child". This process is also called check-in at "parent".

[0024] When this check-in/check-out process is simply implemented by the conventional LCM 1, the following "attack" is present in practice. More specifically, "child" stored in the MC 13 is saved in another recording medium (by removing its MID), and "child" in the MC 13 checks in at "parent". The previously saved "child" is written back to that MC 13. Since check-in has already been done, "parent" on the LCM 1 can copy "child" on another MC 13. This method can form an arbitrary number of "children" that can be used.

[0025] The aforementioned "attack" can be defended by authentication in data transfer between the MC 13 and LCM 1. That is, assume that the MC 13 does not accept data transfer from an LCM other than an authentic LCM 1, and the LCM 1 does not accept data transfer from an MC other than an authentic MC 13. In this case, "child" in the MC 13 cannot be saved in another recording medium. Also, disguised check-in cannot be done at the LCM 1. Therefore, the aforementioned "attack" is no longer effective.

[0026] However, the check-in/check-out process cannot be implemented even under the premise of authentication between the LCM 1 and MC 13, because of the presence of the following "attack". That is, before "parent" on the LCM 1 forms any "child", data of the LCM 1 (especially, information in the license memory 9) is backed up to another recording medium. After "child" is copied to the MC 13, the backed-up data of the LCM 1 is restored. Since "parent" of the LCM 1 recovers the state before it forms "child", it can form "child" on another MC 13. In this manner, an arbitrary number of "children" can be formed.

[0027] In order to implement the check-in/check-out process that can defend such attack, an area (secret area) which cannot be accessed by a public procedure is assured on the storage area of the MC 13, and is used to record information required for mutual authentication and information required for contents decryption, an identification information (device ID) list (revocation list (RVC list)) of devices (LCM 1, PD 12) that cannot be accessed, and the like (see FIG. 2). Also, an area (secret area) that can be accessed by only a private procedure is assured on the storage area (e.g., a hard disk (HDD) when the LCM 1 is constituted by a PC) of the LCM 1, and is used to store a guest book (to be described later) (see FIG. 2). Furthermore, an area (secret area) that can be accessed by only a private procedure may also be assured on the storage area of the PD 12, and may be used to record information required for contents decryption (see FIG. 2). Note that an area other than the secret area in the storage area, which can be accessed by a normal procedure, will be referred to as a public area.

[0028] As shown in FIG. 1, the LCM 1 includes a guest book memory 8 assured on the secret area, and a secret area driver 7 for reading data from the secret area after the SMS 2 executes a specific secret procedure for accessing this guest book memory 8.

[0029] As shown in FIG. 4C, the MC 13 includes an identification information memory (ROM) 13b which stores identification information MID of the MC 13, and cannot be externally rewritten and copied, a secret area 13c, a public area (rewritable RAM) 13a, and a switch (SW) 13e which opens a gate to allow access to the secret area 13c only when an authentication unit 13d authenticates and confirms an authentic partner every time the secret area 13c is accessed.

[0030] Note that three different types of MCs 13 can be used in this embodiment. The type of MC 13 which has both identification information MID and the secret area, as shown in FIG. 4C, is called "level 2". The type of MC 13 which does not have any secret area but has identification information MID, as shown in FIG. 4B, is called "level 1". The type of MC 13 which has neither the secret area nor identification information, and has only a public area, as shown in FIG. 4A, is called "level 0". In order to discriminate these types, for example, level 0 can be discriminated from other types by checking the

presence/absence of identification information MID, and levels 1 and 2 can be discriminated based on the format of identification information MID. For example, when identification information is a serial number, a medium having identification information equal to or larger than a predetermined value is determined to be level 2.

[0031] An MC 13 of level 2 will be exemplified below unless otherwise specified.

[0032] The MC 13 is set in the PD 12 connected to the LCM 1 or is directly set in the LCM 1 when it is used.

[0033] FIG. 3 shows an example of the arrangement of the PD 12, and the MC 13 is set in a medium interface (I/F) 12f. When the LCM 1 reads/writes data to/from the MC 13 via the PD 12, it accesses the secret area of the MC 13 via a secret area access unit in the PD 12. The medium I/F 12f includes a secret area access unit for accessing the secret area of the MC 13. The secret area in the PD 12 may be assured on a flash memory 12d. A ROM 12c is written with a mutual authentication program between the MC 13 and LCM 1, a program that describes an authentication procedure required for accessing the secret area, and a program for discriminating the type of MC 13. According to these programs, various processes such as authentication, type discrimination, and the like with the MC 13 are executed under the control of a CPU 12a.

[0034] The ROM 12c may also store identification information (device ID) of the PD 12. For example, the secret area assured on the flash memory 12d pre-stores a secret device ID (SPDID).

[0035] FIG. 5 shows the arrangement of the medium I/F 6 of the LCM 1. The medium I/F 6 includes an authentication unit 6c for performing mutual authentication with the MC 13, a medium discrimination unit 6b for determining the type of MC 13, and a controller 6a for controlling all these units. The authentication unit 6c also serves as a secret area access unit which accesses the secret area of the MC 13.

[0036] The guest book stored in the secret area of the LCM 1 will be explained below.

[0037] All music contents held in the SMS 2 have contents IDs (TIDs) as identification information for identifying the individual contents, and the predetermined number of contents that can be copied, i.e., the remaining number of children and a check-out list as their attribute information. This attribute information is called a guest book. The guest book is recorded on the guest book memory 8 assured on the secret area in the format shown in FIG. 7A.

[0038] Referring to FIG. 7A, the remaining number of children of contents ID = "TID1" is "2" and its check-out list is L1.

[0039] The check-out list is a list of identification information of the MCs 13 which record copied contents (children). For example, as can be seen from check-out list L1 in FIG. 7A, children of the contents having a contents ID = "TID1" are checked out to two MCs 13 respectively having identification information = "m1" and "m2".

[0040] The following items will be explained in turn below.

1. Outline of mutual authentication method
2. Check-in/check-out/reproduction process of copied contents using MC of level 2
3. Check-in/check-out/reproduction process of copied contents using MC of level 0

1. Outline of mutual authentication method

[0041] In order to safely implement the check-in/check-out process, mutual authentication must be done among the LCM 1, PD 12, and MC 13 as described above (to confirm, e.g., if they have an identical algorithm). In general, the mutual authentication process must have secret information shared by the partners which are to authenticate each other. Therefore, for example, the MC 13, LCM 1, and PD 12 have such secret information. In terms of information security, this secret information is preferably a dynamic one which is generated to have a different value every time authentication is done. However, if a high-grade function of generating such secret information is added to the medium itself, i.e., the MC 13, the medium becomes expensive. In order to promote further prevalence of media to public, the medium is preferably as inexpensive as possible. Therefore, secret information is preferably pre-stored in the MC 13 to reduce the cost of the medium (MC 13).

[0042] However, when secret information which is common to all media or a given number of media (such information will be referred to as global secret information hereinafter) is pre-stored in respective media, if the secret information is read from a given medium by some method, other media that store identical secret information may be illicitly used. It is therefore very dangerous to store global secret information in media (see FIG. 8A).

[0043] Even when secret information stored in a given medium is read by an unauthorized user, if it is only the medium from which the secret information has been read that can be illicitly used, no serious problem is posed. For this reason, the secret information need only be unique to each medium.

[0044] In this embodiment, secret information for mutual authentication, which information differs in units of media, is stored in each media, and the LCM 1 or PD 12 and MC 13 perform mutual authentication using the stored information, thereby providing a safe mutual authentication method that uses a low-cost medium and can assure higher security. More specifically, the mutual authentication method described in this embodiment pre-stores, in (the secret area of) each medium (medium of level 2), secret information (in this case, secret medium ID (SMID): which is obtained by encrypting a medium ID using key information K_M acquired by

some method), which differs in units of media and is required for mutual authentication (AKE), and transfers identification information (MID) of that medium to the LCM 1 and PD 12, as shown in FIG. 8B. The LCM 1 or PD 12 generates information (which is the same as SMID of the medium) for mutual authentication) using MID and information (K_M) acquired by some method in accordance with a predetermined algorithm and executes a mutual authentication process (AKE: authentication and key exchange)).

[0045] In this manner, by storing unique secret information (SMID) in each MC 13, the LCM 1 or PD 12 generates secret information (SMID) on the basis of information (MID) unique to each medium, which is transferred from the medium, thereby implementing safe mutual authentication without imposing any heavy load on the medium.

[0046] Note that the mutual authentication process according to the gist of the present invention will be referred to as AKE hereinafter.

[0047] When the MC 13 is set in the medium I/F 6 of the LCM 1 or the PD 12, mutual authentication may be done first between the medium I/F 6 and MC 13 or between the PD 12 and MC 13 (step S1 in FIG. 9). If it is determined that both of them are authentic (e.g., they have hardware arrangements complying with the same standards) (step S2), the medium I/F 6 or PD 12 determines the type of MC 13 on the basis of identification information MID read from the MC 13 (step S3). The medium I/F 6 or PD 12 executes a check-in/check-out/reproduction process according to the determined type (step S6).

[0048] Note that mutual authentication in step S1 in FIG. 9 need not always be that according to the gist of the present invention shown in FIG. 8B.

[0049] In the above description, three different types of MCs 13, i.e., MCs 13 of level 0 to level 2, are available, but the check-in/check-out/reproduction process operations of the copied contents in FIG. 9 and the subsequent figures will be explained for two types of MCs 13, i.e., MCs 13 of level 0 and level 2.

[0050] Furthermore, in accessing each others secret areas between the LCM 1 and MC 13, the LCM 1 and PD 12, and the PD 12 and MC 13, assume that they authenticate each other, open gates to each other's secret areas if it is confirmed that they are authentic, and close the gates that allow access to the secret areas (although not described in the following description) after access to the secret areas is completed. For example, between the LCM 1 and MC 13, the SMS 2 makes mutual authentication with the MC 13 so as to access the secret area 13c of the MC 13. If their authenticity is confirmed and the switch 13e opens the gate to the secret area 13c, the SMS 2 writes key information in the secret area 13c, and the switch 13e closes the gate that allows access to the secret area 13c upon completion of the write.

2. Check-in/check-out/reproduction process of copied contents using MC of level 2

[0051] The check-in/check-out/reproduction process using the MC 13 of level 2 with the format shown in FIG. 4C will be explained below.

[0052] A case will be explained below with reference to FIG. 10 wherein a check-out instruction is issued to the SMS 2 via a user interface (I/F) 15 or via the PD 12 (i.e., when the MC 13 is set in the PD 12 connected to the LCM 1).

[0053] The SMS 2 checks the remaining number n of children of contents (e.g., having a contents ID = "TID1") corresponding to a check-out request of the guest book. If n > 0, the SMS 2 reads out the device ID (LCMID) of the corresponding LCM 1 from the device ID memory 4, and transfers it to the MC 13 (step S101).

[0054] The MC 13 checks if the transferred device ID is registered in the RVC list (step S102). If the transferred device ID is not registered, the MC 13 reads out master key K_M by accessing the secret area 13c, and transfers it to the LCM 1 (step S103). Furthermore, the MC 13 reads out its identification information (MID) from the identification information memory 13b and transfers it to the LCM 1 (step S104).

[0055] The LCM 1 encrypts the medium ID (MID) transferred from the MC 13 using master key K_M to generate information (K_M[MID]) required for a mutual authentication process (AKE) (step S105).

[0056] The LCM 1 executes the mutual authentication process (AKE) using the generated information K_M[MID], while the MC 13 executes the mutual authentication process (AKE) using a secret medium ID (SMID) (step S106). In this mutual authentication process (AKE), the LCM 1 and MC 13 share identical functions g(x, y) and H(x, y), and if the information K_M[MID] generated by the LCM 1 is the same as the secret medium ID (SMID) of the MC 13, they can confirm their authenticity by the mutual authentication process (AKE).

[0057] The processing operation of the mutual authentication process (AKE) in step S106 will be explained below with reference to FIG. 21.

[0058] The LCM 1 generates random number R1 (step S301), and transfers it to the MC 13. At the same time, the LCM 1 substitutes random number R1 in one variable of function g(x, y) having two variables. Also, the LCM 1 substitutes the information K_M[MID] generated in step S105 in FIG. 10 in the other variable of function g(x, y) to obtain the value of function g (step S302).

[0059] On the other hand, the MC 13 substitutes random number R1 transferred from the LCM 1 in one variable of function g(x, y), substitutes its own secret medium ID (SMID) in the other variable, and transfers the obtained value of function g to the LCM 1 (step S303).

[0060] The LCM 1 compares the value of function g

transferred from the MC 13, and that computed by itself, and executes a subsequent process if they match. If the two values do not match, the AKE process on the LCM 1 side is canceled at that time (step S304).

[0061] The MC 13 then generates random number R2 (step S305), and transfers it to the LCM 1. At the same time, the MC 13 substitutes random number R2 in one variable of function g(x, y) having two variables. Also, the MC 13 substitutes its secret medium ID (SMID) in the other variable of function g(x, y) to obtain the value of function g (step S306).

[0062] On the other hand, the LCM 1 substitutes random number R2 transferred from the MC 13 in one variable of function g(x, y), and substitutes the information K_M[MID] generated in step S105 in FIG. 10 in the other variable of function g(x, y) to obtain the value of function g. The LCM 1 then transfers the obtained value to the MC 13 (step S307).

[0063] The MC 13 compares the value of function g transferred from the LCM 1, and that computed by itself, and executes a subsequent process if they match. If the two values do not match, the AKE process on the MC 13 side is canceled at that time (step S308).

[0064] If the values of function g match in step S308, the MC 13 substitutes random number R2 in one variable of function H(x, y) having two variables, and its secret medium ID (SMID) in the other variable to generate key information KT (step S309).

[0065] Also, if the values of function g match in step S304, the LCM 1 substitutes random number R2 transferred from the MC 13 in one variable of function H(x, y), and substitutes the information K_M[MID] generated in step S105 in FIG. 10 in the other variable to generate key information KT (step S310).

[0066] Note that two pieces of key information KT, which are generated by the LCM 1 and MC 13 using the identical function H(x, y) if it is determined in steps S304 and S308 that the values of function g match, are the same ones. The LCM 1 and MC 13 then exchange contents decryption key Kc using this key information KT.

[0067] The mutual authentication process (AKE) preferably generates different key information KT in each authentication in terms of security. In this case, since random number R2 newly generated for each authentication is substituted in one of two variables which are substituted in function H used to generate key information KT, different key information KT can be generated for each authentication.

[0068] Referring back to FIG. 10, if the LCM 1 and MC 13 confirm in step S106 that they are authentic, the MC 13 stores the generated key information KT (in this case, KT1) in the secret area (step S107). The LCM 1 encrypts a decryption key (contents decryption key) Kc used to decrypt the encrypted contents (KT1[Kc]) using the key information KT1 generated in step S106, and transfers it to the MC 13 (steps S108 and S109). Also, the LCM 1 encrypts contents C using Kc (Kc[C]), and transfers the encrypted contents to the MC 13 (steps S110 and S111).

[0069] Finally, the SMS 2 subtracts "1" from the remaining number n of children of the contents with the contents ID = "TID1" corresponding to the check-out request of the guest book, and adds identification information "m0" of that MC 13 in check-out list L1, as shown in FIG. 7B.

[0070] The MC 13 stores transferred encrypted contents decryption key KT1[Kc] and encrypted contents Kc[C] in the public area 13a.

[0071] FIG. 6 shows the storage contents of the MC 13 at completion of the aforementioned processes.

[0072] A case will be explained below with reference to FIG. 11 wherein a reproduction instruction is issued to the SMS 2 via the user interface (I/F) 15 of the LCM 1 or to the PD 12.

[0073] The PD 12 or LCM 1 transfers its own device ID to the MC 13 (step S121).

[0074] If the LCM 1 has the same contents reproducing function (demodulator 12g, decoder 12h, D/A converter 12i, and the like) as that the PD 12 shown in FIG. 3, the contents of the MC 13 can be similarly reproduced by the PD 12 and LCM 1. A reproduction process by the PD 12 will be exemplified below.

[0075] The MC 13 checks if the transferred device ID is registered in the RVC list (step S122). If the device ID is not registered, the MC 13 reads out master key K_M by accessing the secret area 13c, and transfers it to the PD 12 (step S123). Furthermore, the MC 13 reads out its identification information (MID) from the identification information memory 13b and transfers it to the PD 12 (step S124).

[0076] The PD 12 encrypts the medium ID (MID) transferred from the MC 13 using master key K_M to generate information (K_M[MID]) required for a mutual authentication process (AKE) (step S125).

[0077] The PD 12 executes the mutual authentication process (AKE) using the generated information K_M[MID], while the MC 13 executes the mutual authentication process (AKE) using a secret medium ID (SMID) (step S126). Since the mutual authentication process in step S126 is the same as that shown in FIG. 21, a description thereof will be omitted.

[0078] If the PD 12 and MC 13 confirm that they are authentic, the MC 13 encrypts key information KT1 stored in the secret area 13c using the generated key information KT (in this case, KT2) (KT2[KT1]) and transfers it to the PD 12 (steps S127 and S128). On the other hand, the PD 12 can decrypt KT2[KT1] transferred from the MC 13 using key information KT2 generated in step S126 (step S128).

[0079] The MC 13 reads out encrypted contents decryption key KT1[Kc] and encrypted contents Kc[C] from the public area 13a and transfers them to the PD 12 (steps S129 and S131).

[0080] If key information KT1 has been successfully decrypted, the PD 12 can obtain contents decryption key Kc by decrypting contents decryption key KT1[Kc]

which was encrypted using KT1 (step S130). Accordingly, it decrypts encrypted contents Kc[C] using that contents decryption key Kc to obtain contents C (step S132). In the PD 12, the decoder 12h decodes contents C, and the D/A converter 12i converts the decoded contents from a digital signal into an analog signal, thereby reproducing the copied contents (e.g., music) recorded on the MC 13.

[0081] A case will be explained below with reference to FIG. 12 wherein a check-in instruction is issued to the SMS 2 via the user interface (I/F) 15 of the LCM 1 or via the PD 12 (i.e., when the MC 13 is set in the PD 12 connected to the LCM 1).

[0082] The SMS 2 reads out the device ID (LCMID) of that LCM 1 from the device ID memory 4, and transfers it to the MC 13 (step S141).

[0083] The MC 13 checks if the transferred device ID is registered in the RVC list (step S142). If the transferred device ID is not registered, the MC 13 reads out master key K_M by accessing the secret area 13c, and transfers it to the LCM 1 (step S143). Furthermore, the MC 13 reads out its identification information (MID) from the identification information memory 13b and transfers it to the LCM 1 (step S144).

[0084] The LCM 1 encrypts the medium ID (MID) transferred from the MC 13 using master key K_M to generate information (K_M[MID]) required for a mutual authentication process (AKE) (step S145).

[0085] The LCM 1 executes the mutual authentication process (AKE) using the generated information K_M[MID], while the MC 13 executes the mutual authentication process (AKE) using a secret medium ID (SMID) (step S146).

[0086] The mutual authentication process (AKE) of step S146 in check-in will be explained below with reference to FIG. 22. Note that the same reference numerals denote the same portions as those in FIG. 21, and only different portions will be explained below. That is, in FIG. 22 if it is determined in step S308 that the values of function g match, the value of flag information Fake is set to be "true" (indicated by "T" in FIG. 22) in place of generating key information KT; if they do not match, the value of flag information Fake is set to be "false" (indicated by "F" in FIG. 22) (steps S321 and S322). If the values of function g match in step S304, the LCM 1 outputs only that determination result in place of generating key information KT.

[0087] Referring back to FIG. 12, if the LCM 1 confirms authenticity of the MC 13 in step S146 (step S304 in FIG. 22), it instructs the MC 13 to delete key information KT1 stored in the secret area 13c of the MC 13. Upon receiving this instruction, the MC 13 checks the value of flag information Fake. If Fake = "T", the MC 13 deletes key information KT1 from the secret area 13c, and rewrites flag information Fake to "F" (steps S147 and S148). At this time, the encrypted contents stored in the public area 13a of the MC 13 may be erased by overwriting random numbers generated by the LCM 1 on them.

[0088] Finally, as shown in FIG. 7C, the SMS 2 adds "1" to the remaining number n of the contents with the contents ID = "TID1" corresponding to the check-in request of the guest book, and deletes identification information m0 of that MC 13 from check-out list L1.

[0089] On the other hand, if the value of flag information Fake is "F", the subsequent process is canceled.

[0090] The processing operation in check-out, which is different from that shown in FIG. 10, will be described below with reference to FIG. 13. Note that the same reference numerals denote the same portions as those in FIG. 10, and only different portions will be explained below. That is, FIG. 13 is characterized by a process for contents decryption key Kc to be transferred to the MC 13.

[0091] Referring to FIG. 13, the LCM 1 encrypts contents decryption key Kc using K_M[MID] (to be expressed by w hereinafter) generated in step S105 (step S162). The LCM 1 further encrypts contents decryption key Kc encrypted by w (w[Kc]) using key information KT1 generated in the mutual authentication process (AKE) in step S106 (KT1[w[Kc]]), and then transfers it to the MC 13 (step S163).

[0092] The MC 13 decrypts the transferred KT1[w[Kc]] using key information KT1 generated in the mutual authentication process (AKE) in step S106 to obtain w[Kc], and stores it in the secret area 13c (step S164).

[0093] Contents C are encrypted using Kc (step S165), and are then transferred to the MC 13 (step S166) as in FIG. 10.

[0094] The reproduction process corresponding to the check-out process shown in FIG. 13 will be explained below with reference to FIG. 14. Note that the same reference numerals denote the same portions as those in FIG. 11, and only different portions will be explained below. More specifically, in FIG. 14 the MC 13 encrypts encrypted contents decryption key w[Kc] stored in the secret area 13c using key information KT2 generated in the mutual authentication process (AKE) in step S126 (KT2[w[Kc]]), and then transfers it to the LCM 1 or PD 12 (step S172). The LCM 1 or PD 12 decrypts KT2[w[Kc]] transferred from the MC 13 using key information KT2 generated in step S126 (step S173), and decrypts the obtained w[Kc] using w = K_M[KID] generated in step S123 to obtain contents decryption key Kc (step S174). The LCM 1 or PD 12 decrypts encrypted contents Kc[C] using this contents decryption key Kc to obtain contents C (step S175). In the LCM 1 or PD 12, the decoder 12h decodes contents C, and the D/A converter 12i converts the decoded contents from a digital signal into an analog signal, thereby reproducing the copied contents (e.g., music) recorded on the MC 13.

[0095] The check-in process corresponding to the check-out process shown in FIG. 13 is substantially the same as that described with reference to FIG. 12, except that contents decryption key w[Kc] encrypted by

w = K_M[MID] is deleted from the secret area 13c of the MC 13 in step S148 in place of key information KT1.

3. Check-in/check-out/reproduction process of copied contents using MC of level 0

[0096] The check-in/check-out and reproduction processes using the MC 13 of level 0 with the format shown in FIG. 4A will be explained below.

[0097] In this case, the MC 13 is set in the PD 12, and executes a check-out process with the LCM 1 via the PD 12. The basic operation is the same as that of the MC 13 of level 2. However, in case of level 0, since the MC 13 has neither a secret area nor a medium ID, the PD 12 executes a process shown in FIG. 10 with respect to the LCM 1 in place of the MC 13 of level 0. For this purpose, the secret area of the PD 12 prestores master key K_M, secret device key SPDID, and a revocation list (RVC list). Note that master key K_M need only have the same function as that of master key K_M stored in the MC 13, but data itself need not be the same.

[0098] In step S3 in FIG. 9, the type of MC 13 is determined to be level 0.

[0099] A case will be explained below with reference to FIG. 15 wherein a check-out instruction is issued to the SMS 2 via a user interface (I/F) 15 or via the PD 12.

[0100] The SMS 2 checks the remaining number n of children of contents (e.g., having a contents ID = "TID1") corresponding to a check-out request of the guest book. If n > 0, the SMS 2 reads out the device ID (LCMID) of the corresponding LCM 1 from the device ID memory 4, and transfers it to the PD 12 (step S201).

[0101] The PD 12 checks if the transferred device ID is registered in the RVC list (step S202). If the transferred device ID is not registered, the PD 12 reads out master key K_M by accessing its secret area, and transfers it to the LCM 1 (step S203). Furthermore, the PD 12 reads out its identification information, i.e., the device ID (PDID) from, e.g., the ROM 12c, and transfers it to the LCM 1 (step S204).

[0102] The LCM 1 encrypts the device ID (PDID) transferred from the PD 12 using master key K_M to generate information (K_M[PDID]) required for a mutual authentication process (AKE) (step S205).

[0103] The LCM 1 executes the mutual authentication process (AKE) using the generated information K_M[PDID], while the PD 12 executes the mutual authentication process (AKE) using a secret device ID (SPDID) (step S206). Since the mutual authentication process in step S206 is the same as that shown in FIG. 21, a description thereof will be omitted.

[0104] If the LCM 1 and MC 13 confirm that they are authentic, the PD 12 stores the generated key information KT (in this case, KT1) in the secret area (step S207). The LCM 1 encrypts a decryption key (contents decryption key) Kc used to decrypt the encrypted contents (KT1[Kc]) using the key information KT1 generated in step S206, and transfers it to the MC 13 via the PD 12 (steps S208 and S209). Also, the LCM 1 encrypts contents C using Kc (Kc[C]), and transfers the encrypted contents to the MC 13 via the PD 12 (steps S210 and S211).

[0105] Finally, the SMS 2 subtracts "1" from the remaining number n of children of the contents with the contents ID = "TID1" corresponding to the check-out request of the guest book, and adds identification information "m0" of that MC 13 in check-out list L1, as shown in FIG. 7B.

[0106] The MC 13 stores transferred encrypted contents decryption key KT1[Kc] and encrypted contents Kc[C] in the public area 13a.

[0107] FIG. 6 shows the storage contents of the MC 13 at completion of the aforementioned processes.

[0108] The processing operation between the PD 12 and MC 13 when the PD 12 receives a reproduction instruction will be explained below with reference to FIG. 16.

[0109] The MC 13 transfers encrypted contents decryption key KT1[Kc] recorded on its public area to the PD 12 (step S221). If the PD 12 is the one which was used to check out the contents to be reproduced with respect to the MC 13, it must store key information KT1 for decrypting the encrypted contents decryption key in its secret area (see step S207 in FIG. 15). Therefore, such authentic PD 12 can obtain contents decryption key Kc by decrypting KT1[Kc] transferred from the MC 13 using key information KT1 read out from its secret area (step S222). Furthermore, the PD can obtain contents C by decrypting encrypted contents KC[C] transferred from the MC 13 using that contents decryption key Kc (steps S223 and S224). In the PD 12, the decoder 12h decodes contents C, and the D/A converter 12i converts the decoded contents from a digital signal into an analog signal, thereby reproducing the copied contents (e.g., music) recorded on the MC 13.

[0110] A case will be explained below with reference to FIG. 17 wherein a check-in instruction is issued to the SMS 2 via the PD 12 (i.e., using the MC 13 set in the PD 12 connected to the LCM 1). In this case as well, the PD 12 executes a process shown in FIG. 12 with respect to the LCM 1 in place of the MC 13 of level 0 as in the check-out process.

[0111] The SMS 2 reads out the device ID (LCMID) of that LCM 1 from the device ID memory 4, and transfers it to the PD 12 (step S231).

[0112] The PD 12 checks if the transferred device ID is registered in the RVC list (step S232). If the transferred device ID is not registered, the PD 12 reads out master key K_M by accessing its secret area, and transfers it to the LCM 1 (step S233). Furthermore, the PD 12 reads out its identification information (PDID) and transfers it to the LCM 1 (step S234).

[0113] The LCM 1 encrypts the device ID (PDID) transferred from the PD 12 using master key K_M to gen-

erate information (K_M[PDID]) required for a mutual authentication process (AKE) (step S235).

[0114] The LCM 1 executes the mutual authentication process (AKE) using the generated information K_M[PDID], while the PD 12 executes the mutual authentication process (AKE) using a secret device ID (SPDID) (step S236).

[0115] Since the mutual authentication process (AKE) of step S236 in check-in is substantially the same as that shown in FIG. 22 except that K_M[PDID] replaces K_M[MID], and the secret device ID (SPDID) replaces the secret medium ID (SMID), a description thereof will be omitted.

[0116] If the LCM 1 confirms authenticity of the PD 12 in step S236 (step S304 in FIG. 22), it instructs the PD 12 to delete key information KT1 stored in its secret area. Upon receiving this instruction, the PD 12 checks the value of flag information Fake. If Fake = "T", the PD 12 deletes key information KT1 from its secret area, and rewrites flag information Fake to "F" (steps S237 and S238). At this time, the encrypted contents stored in the public area 13a of the MC 13 may be erased by overwriting random numbers generated by the LCM 1 on them.

[0117] Finally, as shown in FIG. 7C, the SMS 2 adds "1" to the remaining number n of the contents with the contents ID = "TID1" corresponding to the check-in request of the guest book, and deletes identification information m0 of that MC 13 from check-out list L1.

[0118] On the other hand, if the value of flag information Fake is "F", the subsequent process is canceled.

[0119] The processing operation in check-out, which is different from that shown in FIG. 15, will be described below with reference to FIG. 18. Note that the same reference numerals denote the same portions as those in FIG. 15, and only different portions will be explained below. That is, FIG. 18 is characterized by a process for contents decryption key Kc to be transferred to the PD 12, as in FIG. 13.

[0120] Referring to FIG. 18, the LCM 1 encrypts contents decryption key Kc using K_M[PDID] (to be expressed by w hereinafter) generated in step S205 (step S252). The LCM 1 further encrypts contents decryption key Kc encrypted by w (w[Kc]) using key information KT1 generated in the mutual authentication process (AKE) in step S251 (KT1[w[Kc]]), and then transfers it to the PD 12 (step S253).

[0121] The PD 12 decrypts the transferred KT1[w[Kc]] using key information KT1 generated in the mutual authentication process (AKE) in step S251 to obtain w[Kc], and stores it in the secret area (step S254).

[0122] Contents C are encrypted using Kc (step S255), and are then transferred to the MC 13 via the PD 12 (step S256), as in FIG. 15.

[0123] The reproduction process corresponding to the check-out process shown in FIG. 18 will be explained below with reference to FIG. 19. Note that the same reference numerals denote the same portions as those in FIG. 18, and only different portions will be explained below. More specifically, in FIG. 19 the PD 12 can obtain contents decryption key Kc by decrypting encrypted contents decryption key w[Kc] stored in its secret area using its secret device ID (SPDID = w) (step S261). The PD 12 can obtain contents C by decrypting encrypted contents Kc[C] transferred from the MC 13 using that contents decryption key Kc (step S262). In the PD 12, decoder 12h decodes contents C, and the D/A converter 12i converts the decoded contents from a digital signal into an analog signal, thereby reproducing the copied contents (e.g., music) recorded on the MC 13.

[0124] The check-in process corresponding to the check-out process shown in FIG. 18 will be described below with reference to FIG. 20. Note that the description of FIG. 20 is substantially the same as that of FIG. 17, except that contents decryption key w[Kc] encrypted by w = K_M[PDID] is deleted from the secret area of the PD 12 in step S238 in place of key information KT1.

[0125] As described in detail above, according to the present invention, safe mutual authentication with high security can be implemented using a low-cost recording medium.

Claims

1. A mutual authentication method for use between a recording apparatus which records copied contents on a recording medium having an arithmetic processing function, and the recording medium, said method characterized by comprising the steps of:

   storing in the recording medium at least first information (MID) which depends on the recording medium, and second information (SMID) which is to be shared by the recording apparatus in executing mutual authentication with the recording apparatus and depends on the recording medium; and
   generating by the recording apparatus authentication information (K_M[MID]) used in mutual authentication with the recording medium on the basis of the first information (MID) obtained from the recording medium, and executing mutual authentication between the recording apparatus and the recording medium using the generated authentication information (K_M[MID]) and the second information (SMID).

2. A mutual authentication method for use between a reproducing apparatus which reproduces copied contents recorded on a recording medium having an arithmetic processing function, and the recording medium, said method characterized by comprising the steps of:

storing in the recording medium at least first information (MID) which depends on the recording medium, and second information (SMID) which is to be shared by the reproducing apparatus in executing mutual authentication with the reproducing apparatus and depends on the recording medium; and

generating by the reproducing apparatus authentication information (K_M[MID]) used in mutual authentication with the recording medium on the basis of the first information (MID) obtained from the recording medium, and executing mutual authentication between the reproducing apparatus and the recording medium using the generated authentication information (K_M[MID]) and the second information (SMID).

3. The method according to claim 1 or 2, characterized by characterized by further comprising the step of:

generating the authentication information (K_M[MID]) by encrypting the first information (MID) using an encryption key (K_M) obtained from the recording medium.

4. A recording apparatus for recording copied contents on a recording medium while limiting the number of copied contents to be recorded on the recording medium, said apparatus characterized by comprising:

generation means for generating authentication information (K_M[MID]), which is used in mutual authentication with the recording medium and is to be shared by the recording medium, on the basis of first information (MID) which is obtained from the recording medium and depends on the recording medium; and

mutual authentication means for executing mutual authentication with the recording medium using the authentication information (K_M[MID]) generated by said generation means.

5. A reproducing apparatus for reproducing copied contents recorded on a recording medium while limiting the number of copied contents to be recorded on the recording medium, said apparatus characterized by comprising:

generation means for generating authentication information (K_M[MID]), which is used in mutual authentication with the recording medium and is to be shared by the recording medium, on the basis of first information (MID) which is obtained from the recording medium and depends on the recording medium; and

mutual authentication means for executing mutual authentication with the recording medium using the authentication information (K_M[MID]) generated by said generation means.

6. An apparatus according to claim 4 or 5, characterized in that said generation means generates the authentication information (K_M[MID]) by encrypting the first information (MID) using an encryption key (K_M) obtained from the recording medium.

7. A recording medium having an arithmetic processing function, characterized by comprising:

storage means for pre-storing first information (MID) which is unique to said recording medium, and second information (SMID) which is to be shared by a recording apparatus for recording copied contents on said recording medium and a reproducing apparatus for reproducing the copied contents in executing mutual authentication among the recording medium, the recording apparatus, and the reproducing apparatus, and depends on said recording medium; and

mutual authentication means for executing mutual authentication between the recording medium and the recording apparatus, and between the recording medium and the reproducing apparatus using authentication information (K_M[MID]) generated based on the first information (MID) by the recording apparatus and the reproducing apparatus, and the second information (SMID).

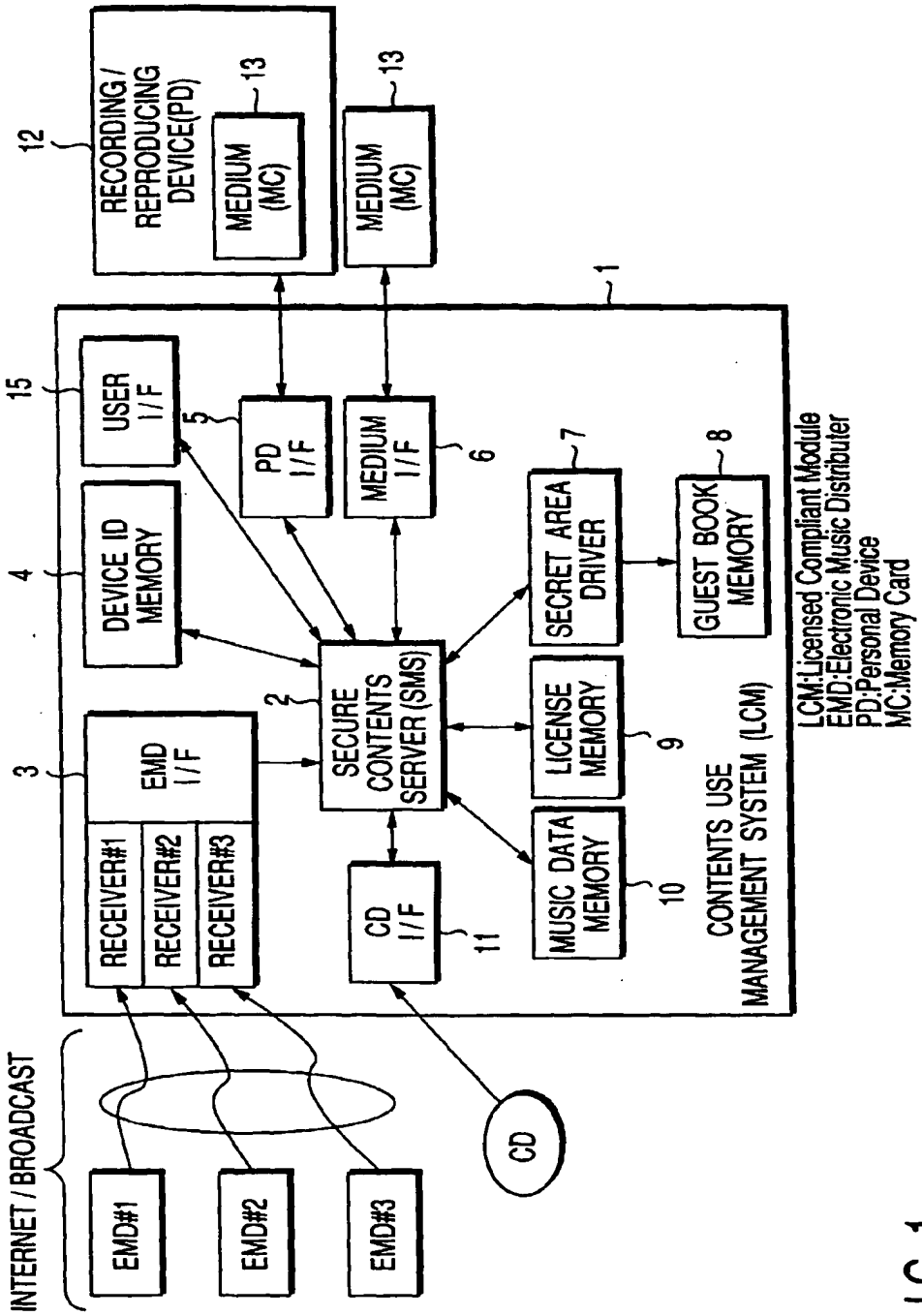
INTERNET / BROADCAST
EMD#1
EMD#2
EMD#3
CD
RECEIVER#1
RECEIVER#2
RECEIVER#3
EMD I/F
3
CD I/F
11
SECURE CONTENTS SERVER (SMS)
2
DEVICE ID MEMORY
4
USER I/F
15
PD I/F
5
MEDIUM I/F
6
MUSIC DATA MEMORY
10
LICENSE MEMORY
9
SECRET AREA DRIVER
7
GUEST BOOK MEMORY
8
CONTENTS USE MANAGEMENT SYSTEM (LCM)
1
RECORDING / REPRODUCING DEVICE(PD)
12
MEDIUM (MC)
13
MEDIUM (MC)
13
LCM:Licensed Compliant Module
EMD:Electronic Music Distributer
PD:Personal Device
MC:Memory Card

FIG. 1

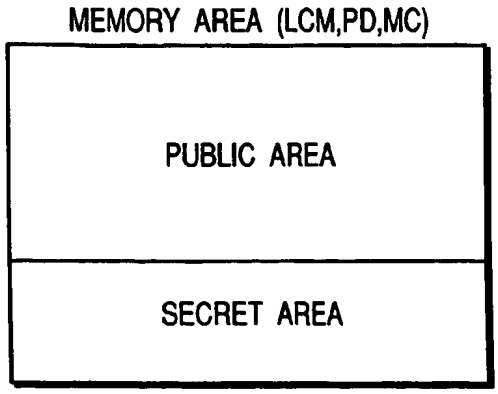
MEMORY AREA (LCM,PD,MC)
PUBLIC AREA
SECRET AREA

FIG. 2

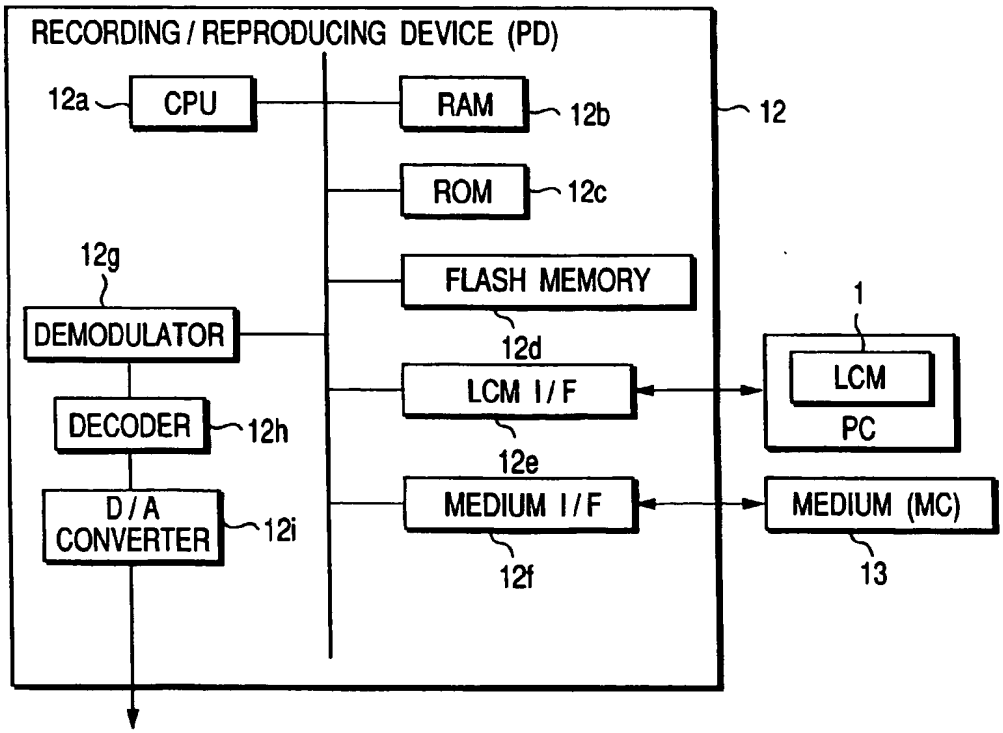
RECORDING / REPRODUCING DEVICE (PD)
12a
CPU
RAM
12b
12
ROM
12c
12g
FLASH MEMORY
1
DEMODULATOR
12d
LCM
LCM I / F
PC
DECODER
12h
12e
D / A CONVERTER
12i
MEDIUM I / F
MEDIUM (MC)
12f
13

FIG. 3

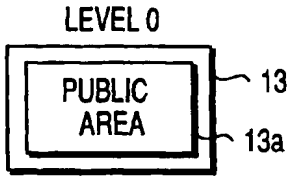

FIG. 4A

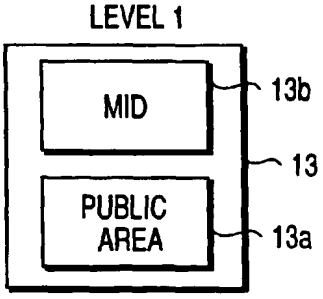

FIG. 4B

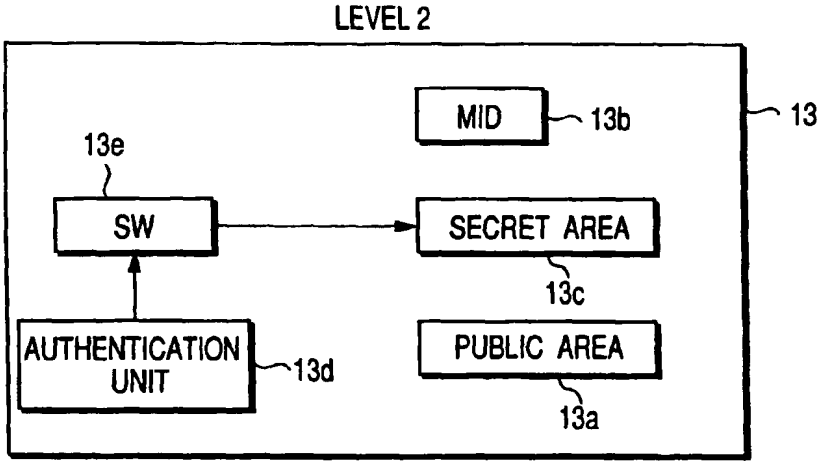

FIG. 4C

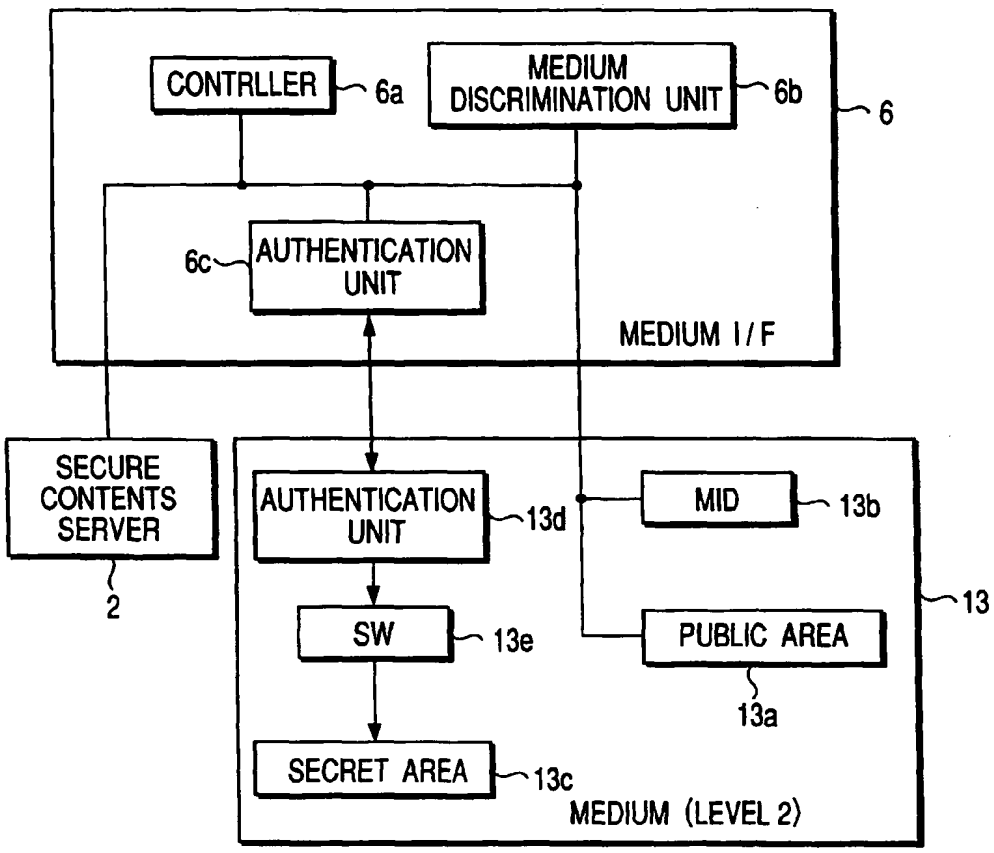
CONTRLLER
6a
MEDIUM DISCRIMINATION UNIT
6b
6
6c
AUTHENTICATION UNIT
MEDIUM I/F
SECURE CONTENTS SERVER
2
AUTHENTICATION UNIT
13d
MID
13b
SW
13e
PUBLIC AREA
13a
13
SECRET AREA
13c
MEDIUM (LEVEL 2)

FIG. 5

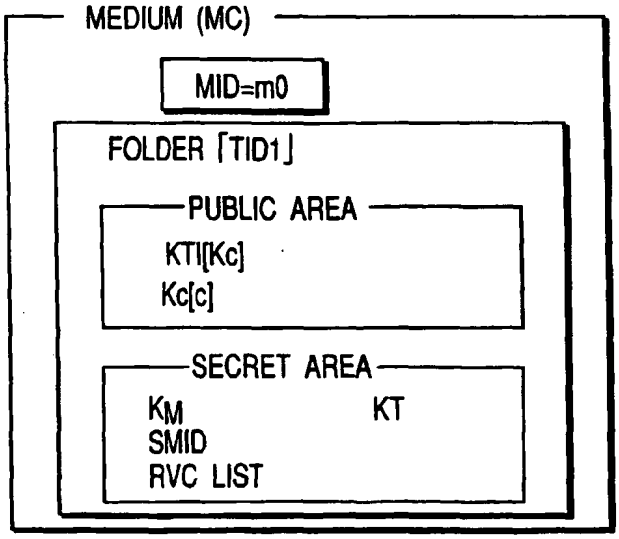
MEDIUM (MC)
MID=m0
FOLDER [TID1]
PUBLIC AREA
KTI[Kc]
Kc[c]
SECRET AREA
KM
KT
SMID
RVC LIST

FIG. 6

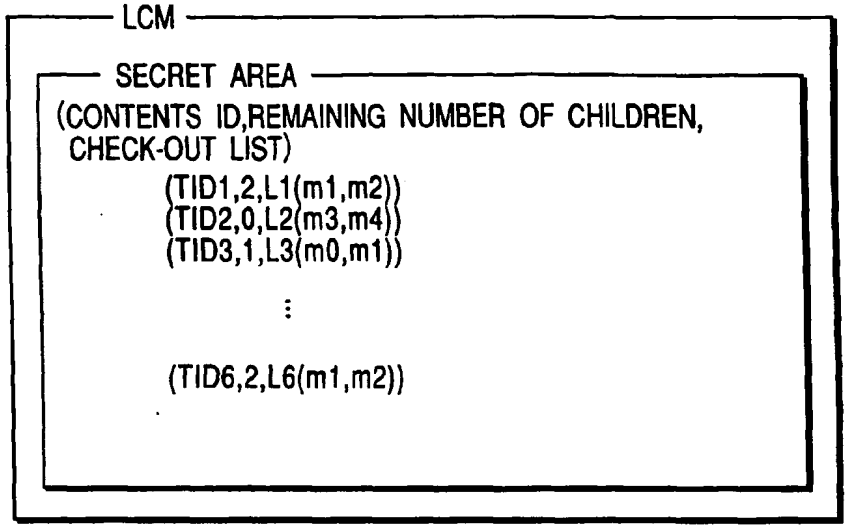

FIG. 7A

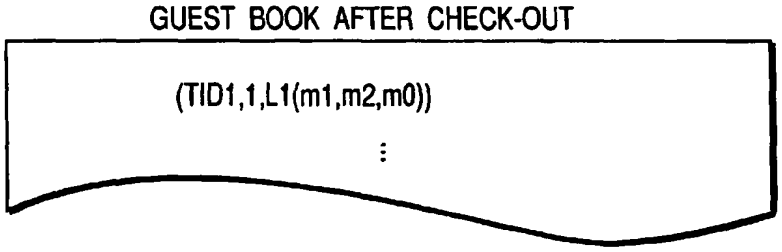

FIG. 7B

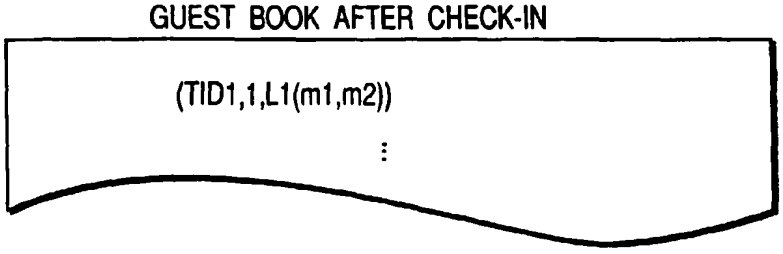

FIG. 7C

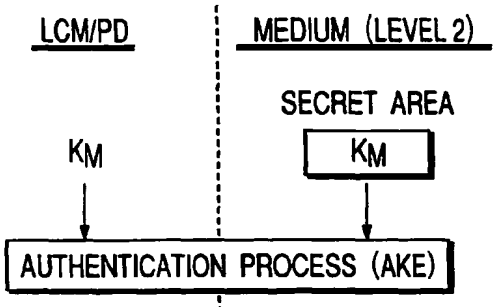

FIG. 8A

KM : GLOBAL SECRET INFORMATION (SECRET INFORMATION COMMON TO GIVEN NUMBER OF MEDIA)

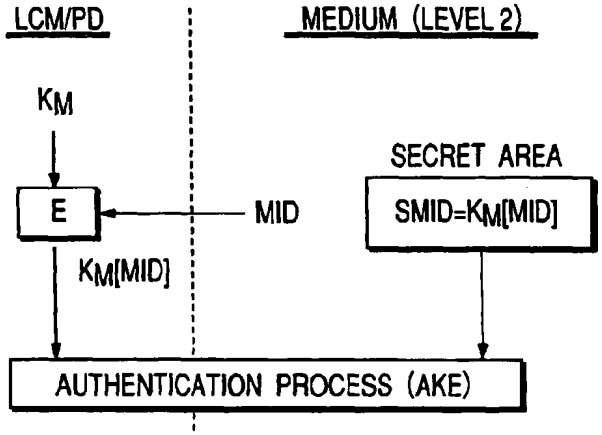

FIG. 8B

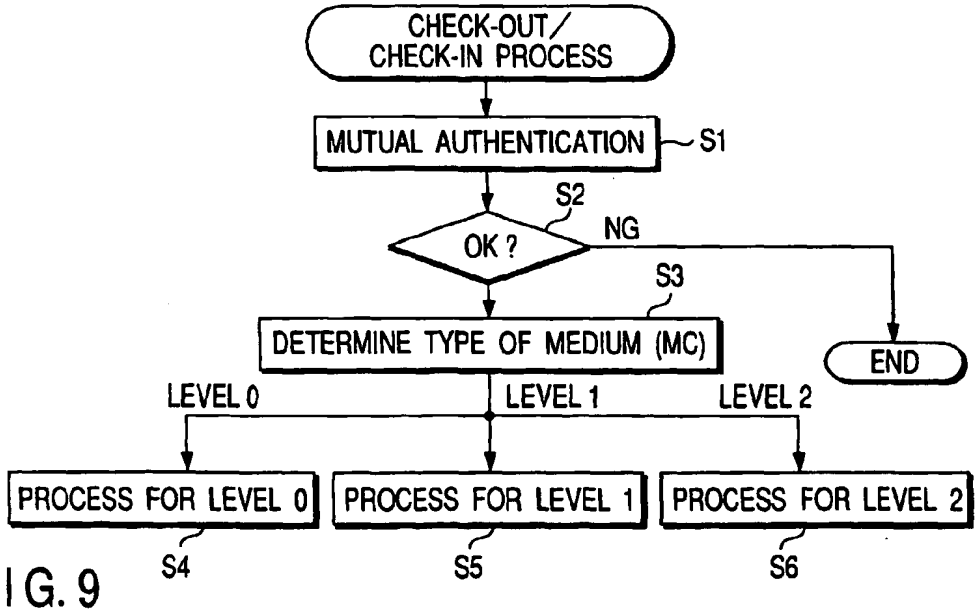

FIG. 9

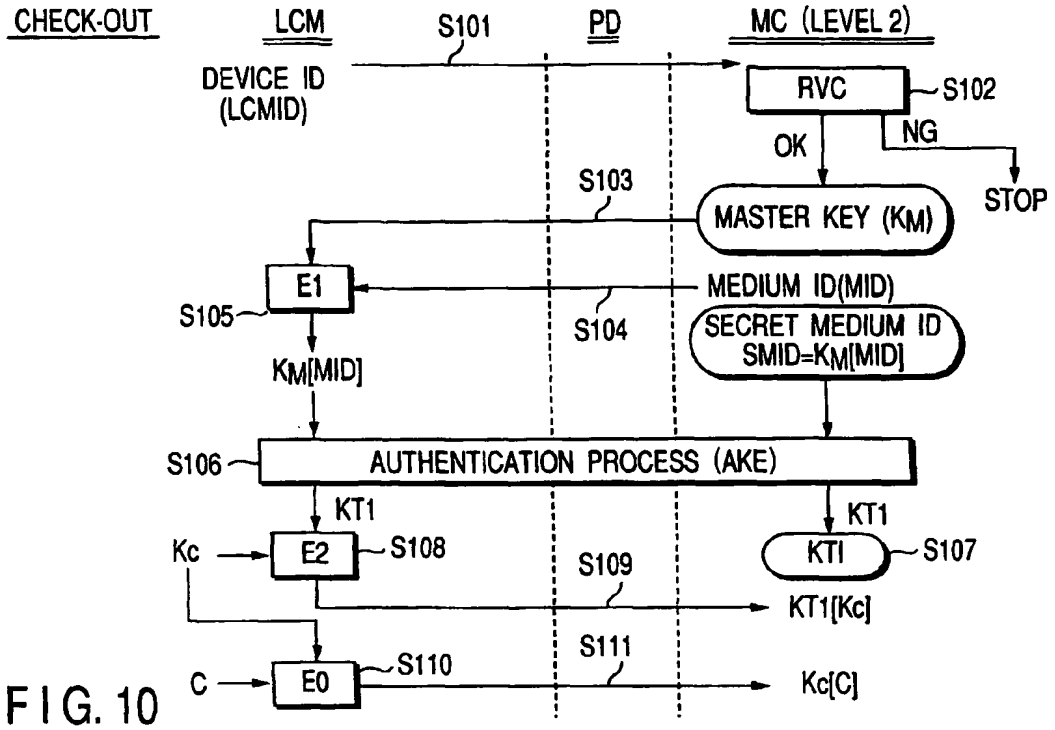
CHECK-OUT
LCM
S101
PD
MC (LEVEL 2)
DEVICE ID (LCMID)
RVC
S102
NG
OK
STOP
S103
MASTER KEY (KM)
E1
MEDIUM ID(MID)
S105
S104
SECRET MEDIUM ID SMID=KM[MID]
KM[MID]
S106
AUTHENTICATION PROCESS (AKE)
KT1
KT1
Kc
E2
S108
KTI
S107
S109
KT1[Kc]
S111
C
E0
S110
Kc[C]

FIG. 10

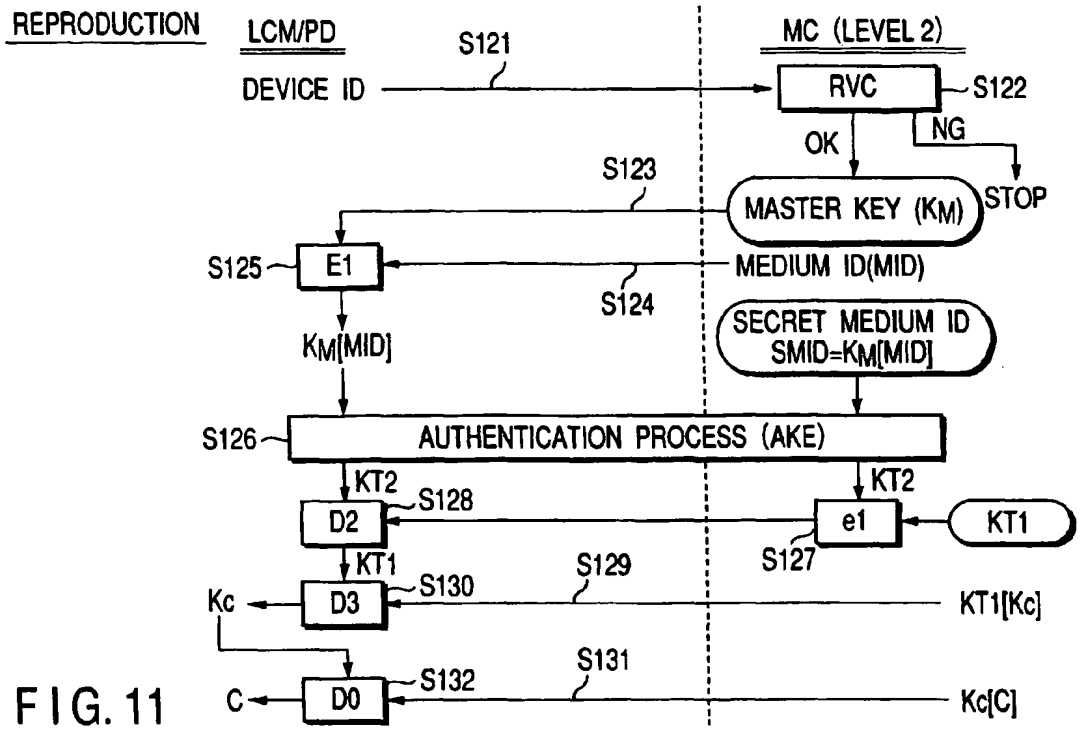
REPRODUCTION
LCM/PD
S121
MC (LEVEL 2)
DEVICE ID
RVC
S122
NG
OK
S123
MASTER KEY (KM)
STOP
S125
E1
MEDIUM ID(MID)
S124
SECRET MEDIUM ID SMID=KM[MID]
KM[MID]
S126
AUTHENTICATION PROCESS (AKE)
KT2
KT2
D2
S128
e1
KT1
S127
KT1
S129
Kc
D3
S130
KT1[Kc]
S131
C
D0
S132
Kc[C]

FIG. 11

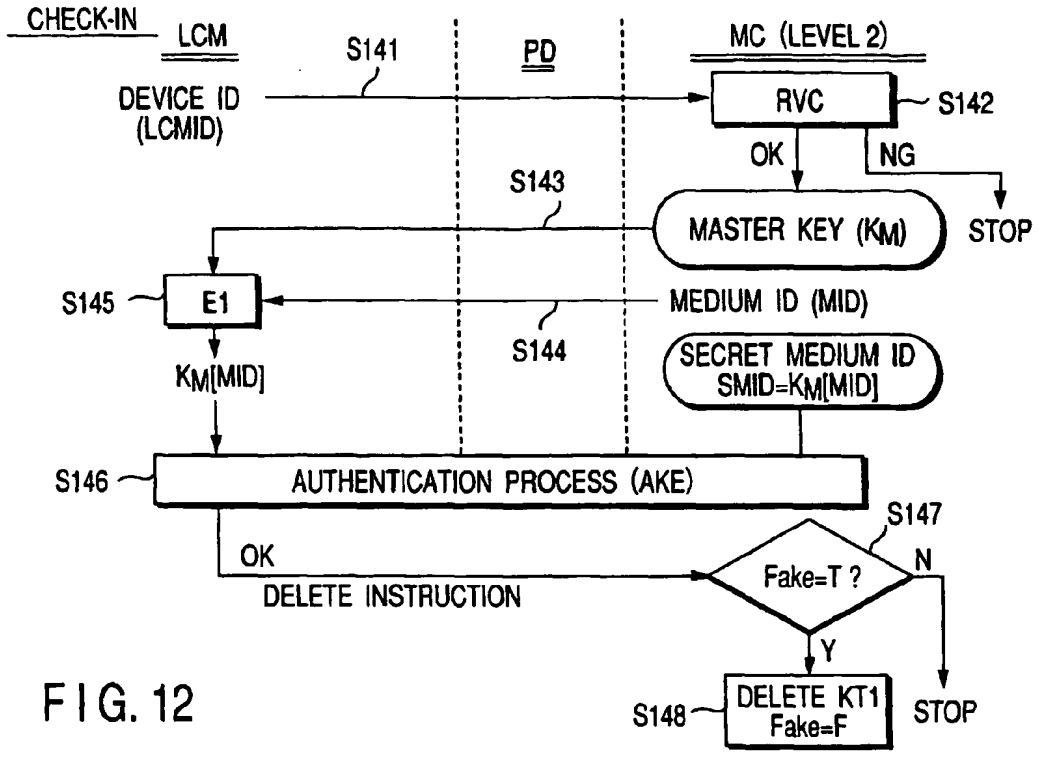
CHECK-IN
LCM
PD
MC (LEVEL 2)
S141
DEVICE ID
(LCMID)
RVC
S142
OK
NG
S143
MASTER KEY (KM)
STOP
S145
E1
MEDIUM ID (MID)
S144
KM[MID]
SECRET MEDIUM ID
SMID=KM[MID]
S146
AUTHENTICATION PROCESS (AKE)
S147
OK
DELETE INSTRUCTION
Fake=T ?
N
Y
S148
DELETE KT1
Fake=F
STOP

FIG. 12

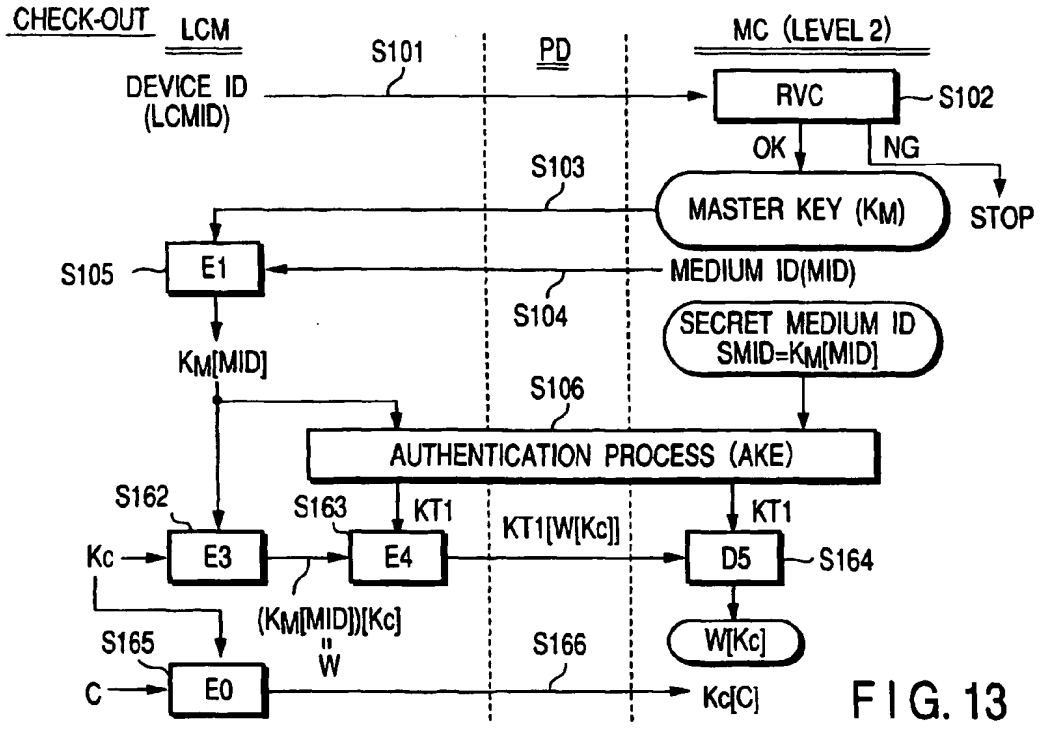
CHECK-OUT
LCM
PD
MC (LEVEL 2)
S101
DEVICE ID
(LCMID)
RVC
S102
OK
NG
S103
MASTER KEY (KM)
STOP
S105
E1
MEDIUM ID(MID)
S104
KM[MID]
SECRET MEDIUM ID
SMID=KM[MID]
S106
AUTHENTICATION PROCESS (AKE)
S162
S163
KT1
KT1[W[Kc]]
KT1
Kc
E3
E4
D5
S164
(KM[MID])[Kc]
=
W
W[Kc]
S165
S166
C
E0
Kc[C]

FIG. 13

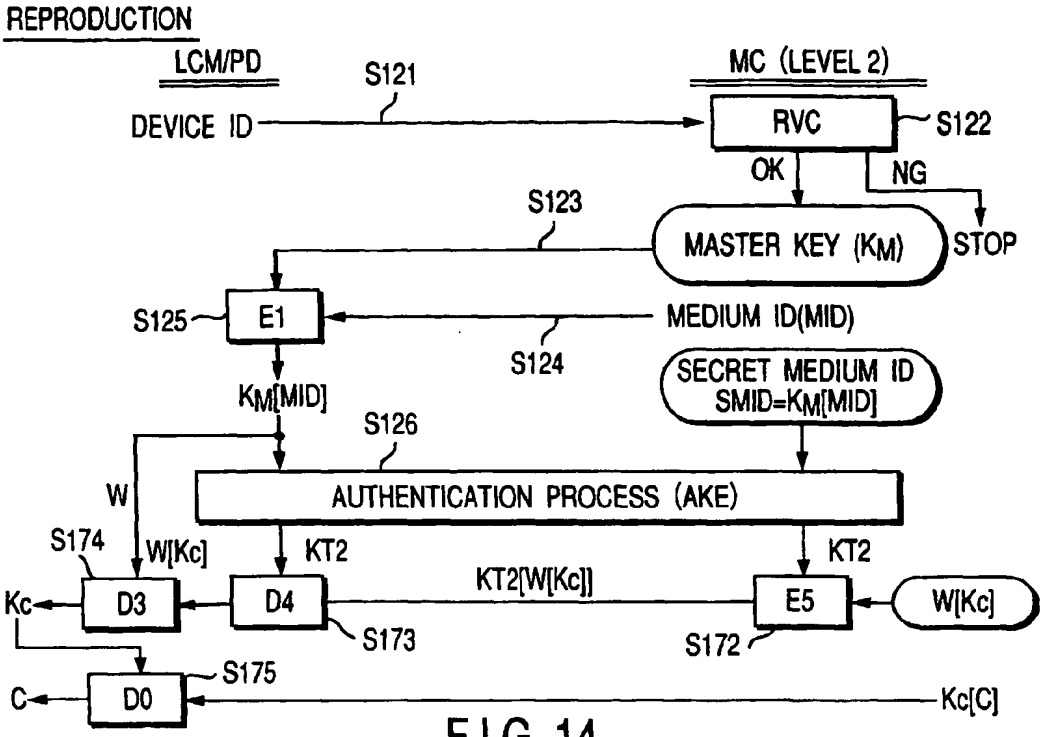
REPRODUCTION
LCM/PD
MC (LEVEL 2)
S121
DEVICE ID
RVC
S122
OK
NG
S123
MASTER KEY (KM)
STOP
S125
E1
MEDIUM ID(MID)
S124
SECRET MEDIUM ID
SMID=KM[MID]
KM[MID]
S126
AUTHENTICATION PROCESS (AKE)
W
S174
W[Kc]
KT2
KT2
KT2[W[Kc]]
Kc
D3
D4
E5
W[Kc]
S173
S172
S175
C
D0
Kc[C]

FIG. 14

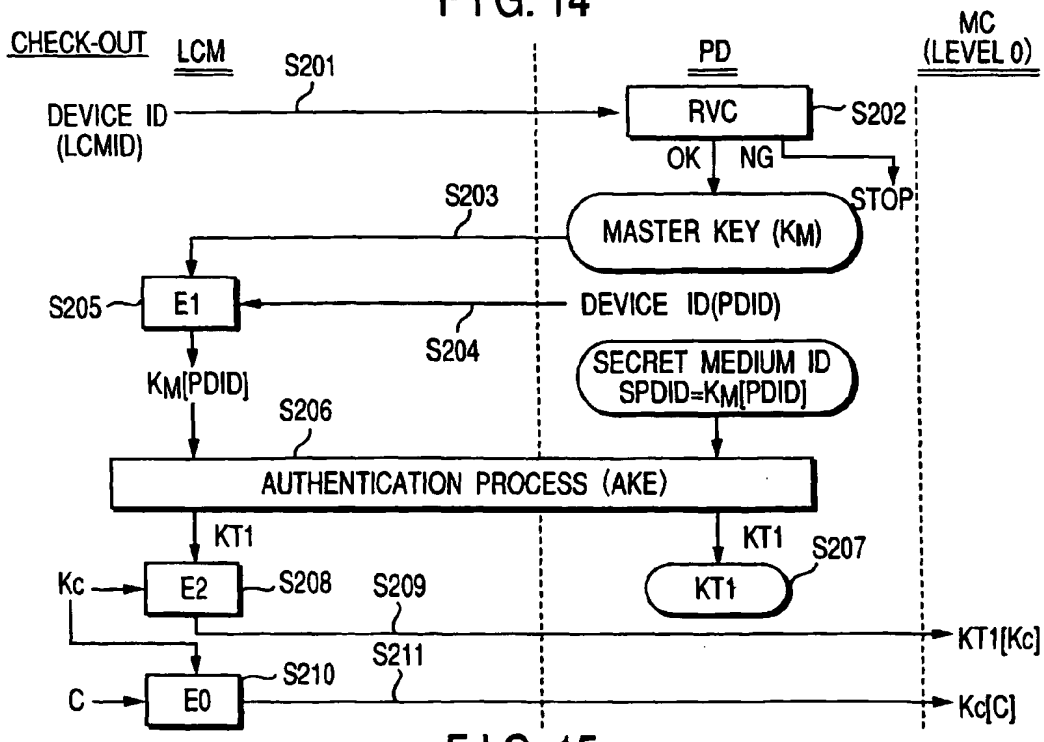
CHECK-OUT
LCM
PD
MC
(LEVEL 0)
S201
DEVICE ID
(LCMID)
RVC
S202
OK
NG
STOP
S203
MASTER KEY (KM)
S205
E1
DEVICE ID(PDID)
S204
KM[PDID]
SECRET MEDIUM ID
SPDID=KM[PDID]
S206
AUTHENTICATION PROCESS (AKE)
KT1
KT1
S207
Kc
E2
S208
S209
KT1
KT1[Kc]
S211
C
E0
S210
Kc[C]

FIG. 15

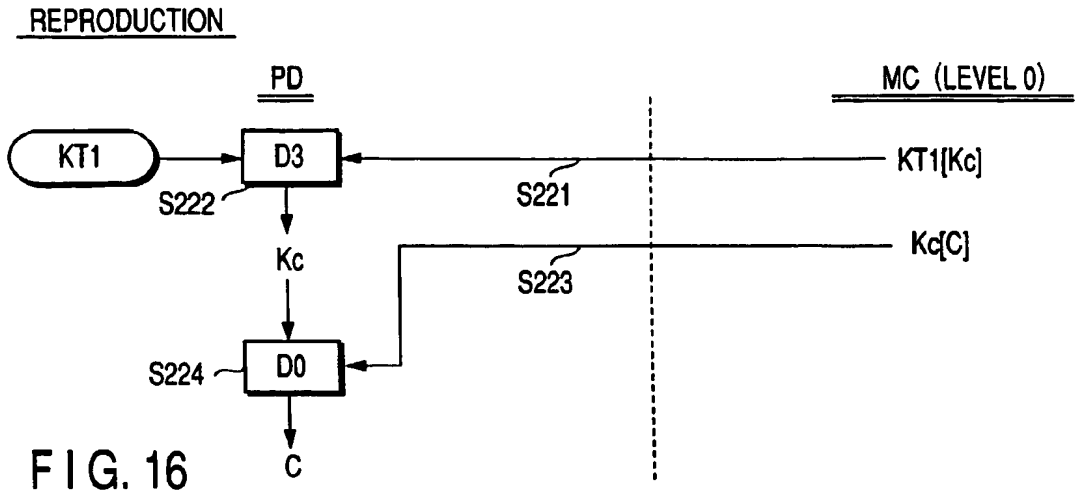
REPRODUCTION
PD
MC (LEVEL 0)
KT1
D3
S222
S221
KT1[Kc]
Kc
S223
Kc[C]
S224
D0
C

FIG. 16

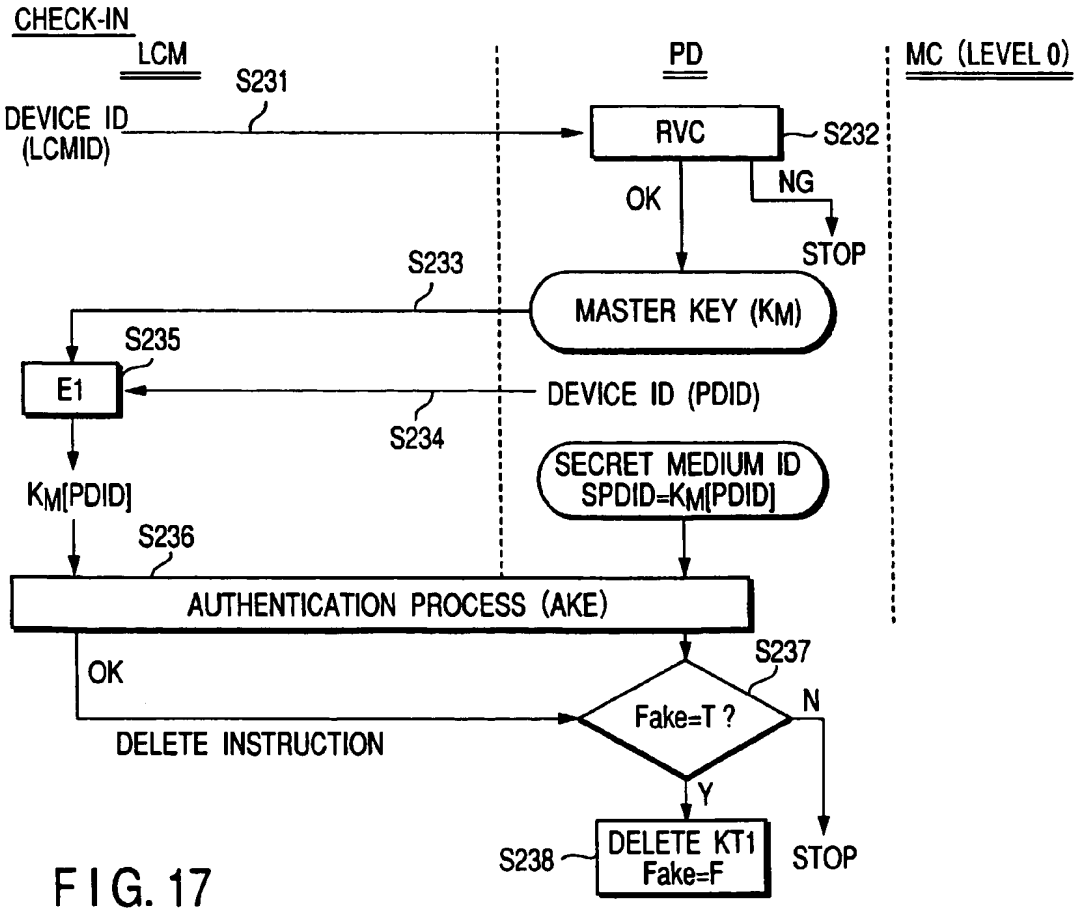
CHECK-IN
LCM
PD
MC (LEVEL 0)
S231
DEVICE ID (LCMID)
RVC
S232
OK
NG
STOP
S233
MASTER KEY (KM)
S235
E1
DEVICE ID (PDID)
S234
SECRET MEDIUM ID SPDID=KM[PDID]
KM[PDID]
S236
AUTHENTICATION PROCESS (AKE)
S237
OK
Fake=T ?
N
DELETE INSTRUCTION
Y
S238
DELETE KT1 Fake=F
STOP

FIG. 17

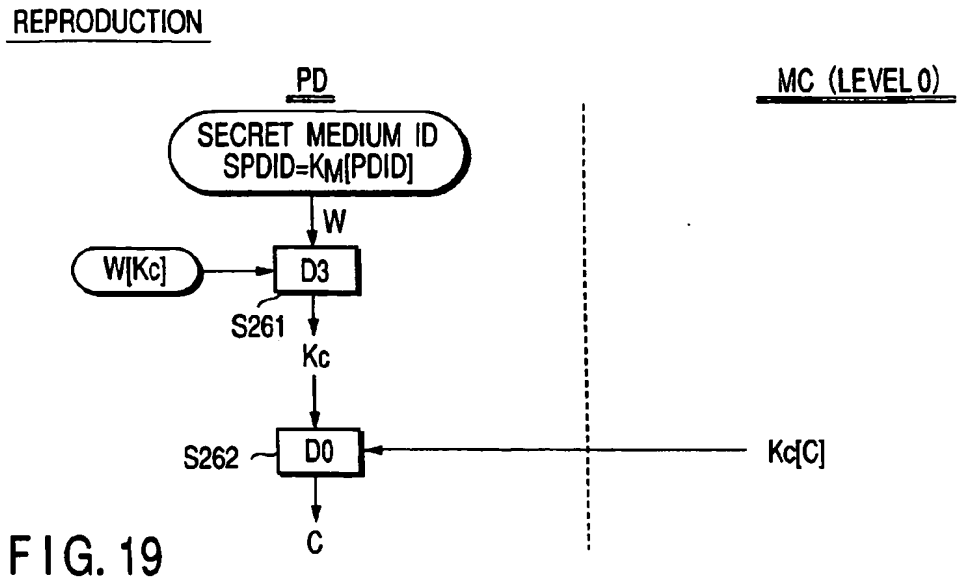
REPRODUCTION
PD
MC (LEVEL 0)
SECRET MEDIUM ID
SPDID=KM[PDID]
W
W[Kc]
D3
S261
Kc
S262
D0
Kc[C]
C

FIG. 19

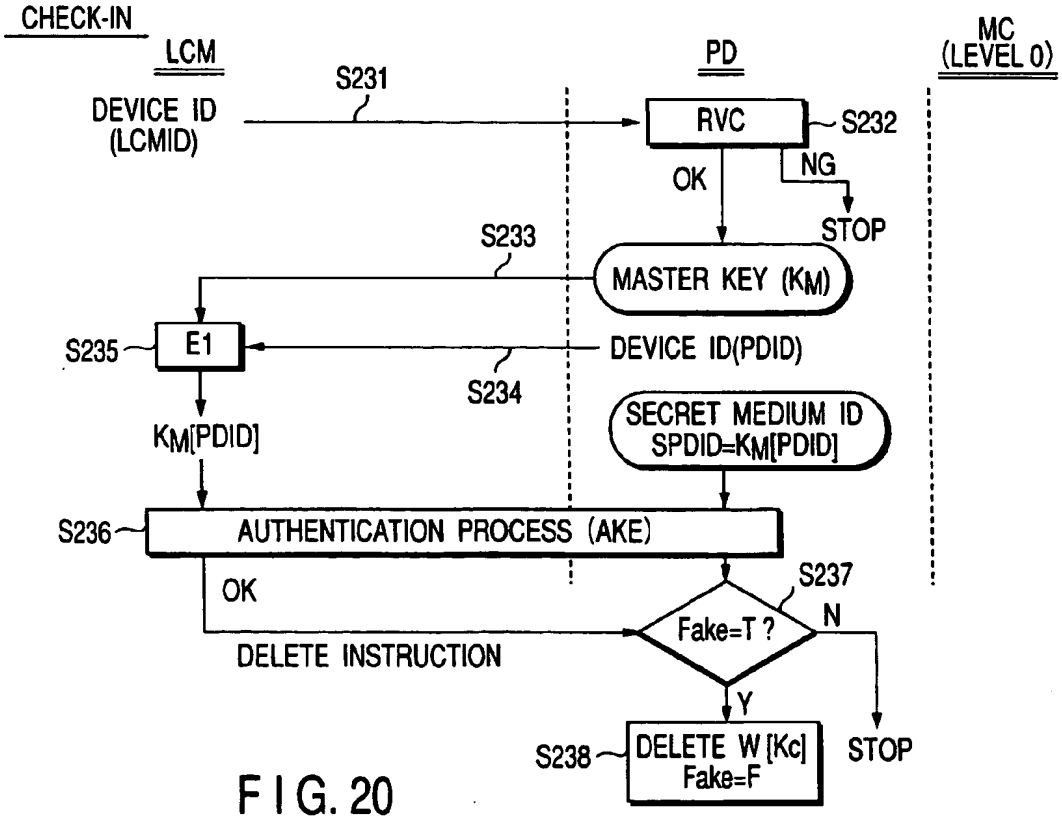
CHECK-IN
LCM
PD
MC
(LEVEL 0)
S231
DEVICE ID
(LCMID)
RVC
S232
OK
NG
STOP
S233
MASTER KEY (KM)
S235
E1
DEVICE ID(PDID)
S234
KM[PDID]
SECRET MEDIUM ID
SPDID=KM[PDID]
S236
AUTHENTICATION PROCESS (AKE)
OK
S237
Fake=T ?
N
DELETE INSTRUCTION
Y
S238
DELETE W [Kc]
Fake=F
STOP

FIG. 20

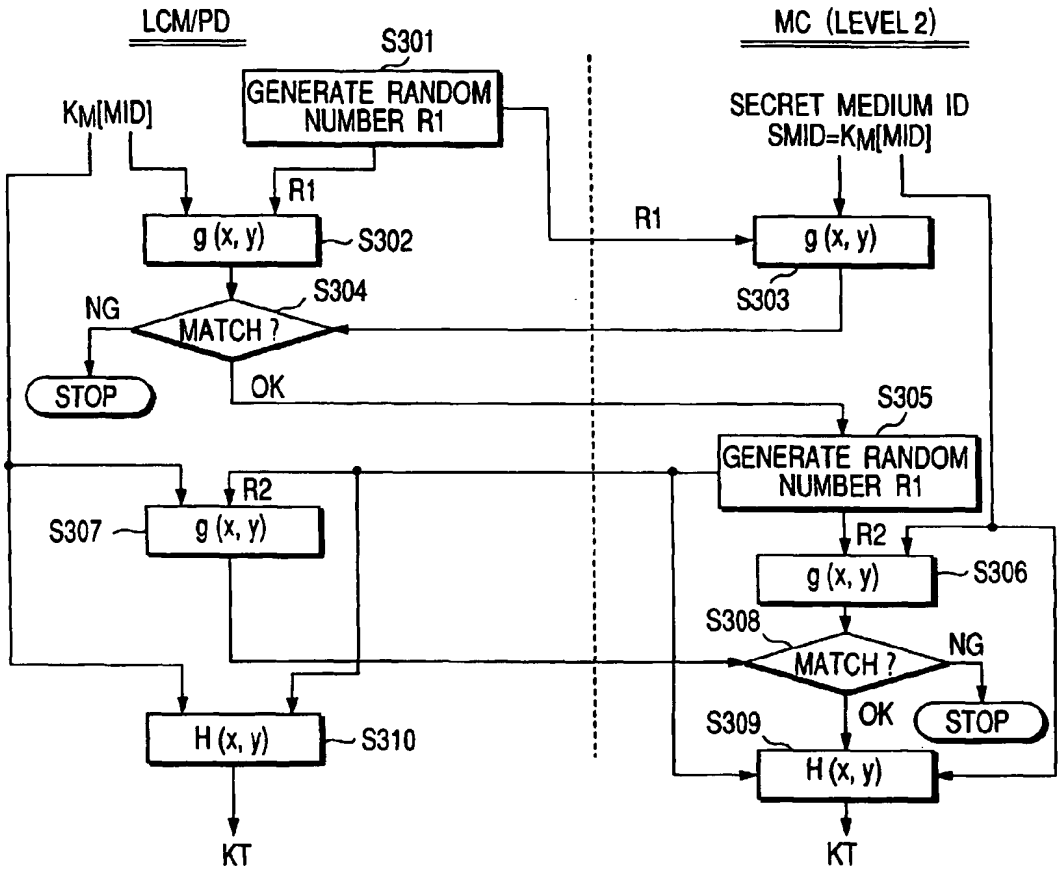
LCM/PD
MC (LEVEL 2)
S301
GENERATE RANDOM NUMBER R1
KM[MID]
SECRET MEDIUM ID
SMID=KM[MID]
R1
g (x, y)
S302
R1
g (x, y)
S303
S304
NG
MATCH ?
STOP
OK
S305
GENERATE RANDOM NUMBER R1
R2
S307
g (x, y)
R2
g (x, y)
S306
S308
MATCH ?
NG
OK
STOP
S309
H (x, y)
S310
H (x, y)
KT
KT

FIG. 21

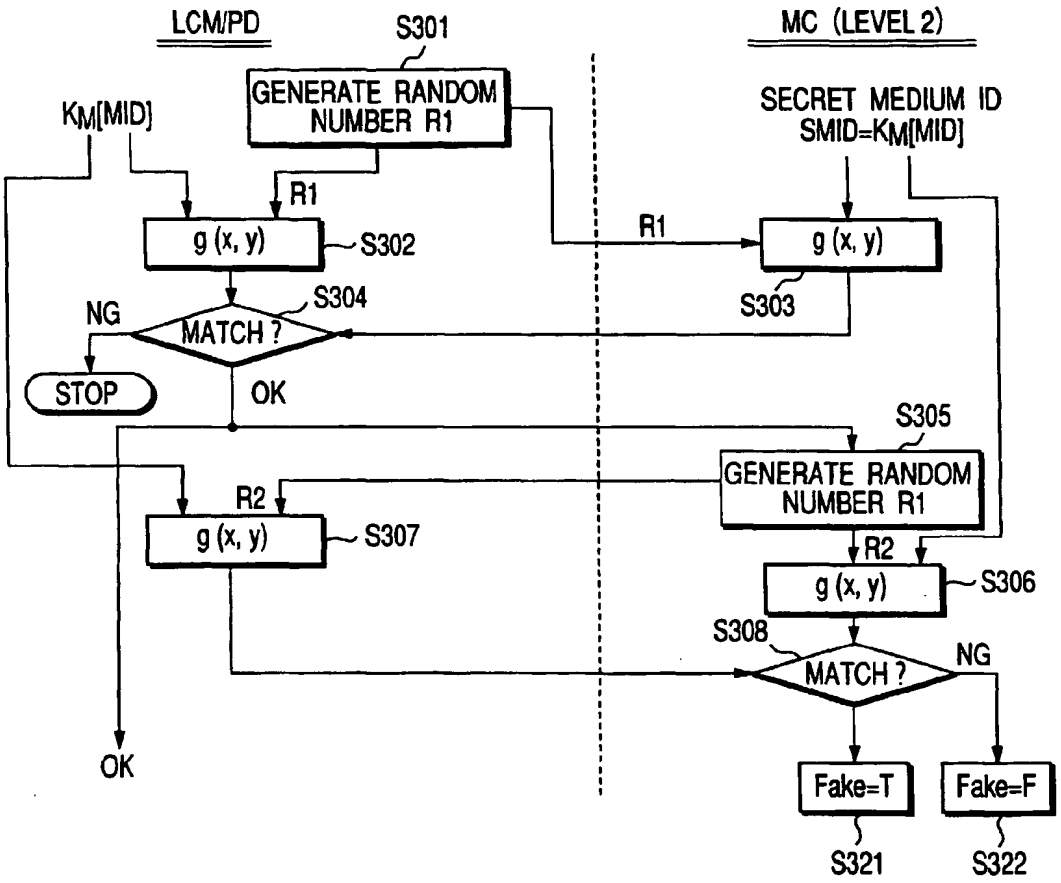
LCM/PD
S301
GENERATE RANDOM NUMBER R1
KM[MID]
R1
g (x, y)
S302
NG
S304
MATCH ?
STOP
OK
R1
MC (LEVEL 2)
SECRET MEDIUM ID
SMID=KM[MID]
g (x, y)
S303
S305
GENERATE RANDOM NUMBER R1
R2
g (x, y)
S306
S308
MATCH ?
NG
R2
g (x, y)
S307
OK
Fake=T
S321
Fake=F
S322

FIG. 22